

RESTORATION OF A COMPUTER TO A PREVIOUS STATE**Publication number:** JP2003503793T**Publication date:** 2003-01-28**Inventor:****Applicant:****Classification:****- international:** **G06F11/14; G06F11/14;** (IPC1-7): G06F9/445;
G06F12/00**- european:** G06F11/14A4B1M2; G06F11/14A4B1M10;
G06F11/14A4C**Application number:** JP20010507196T 20000630**Priority number(s):** US19990141757P 19990630; WO2000US18324
20000630**Also published as:**WO0101285 (A3)
WO0101285 (A2)
WO0101255 (A1)
WO0101255 (A1)
WO0101252 (A1)

more >>

Report a data error he

Abstract not available for JP2003503793T

Abstract of corresponding document: **WO0101251**

Methods and systems for backing up and restoring the state of a computer system are disclosed. Computer resource use is minimized by combining the backup methods of file copying and file logging. During backup, copies are stored of those files that are expected to change frequently. For other files, changes are noted in a change log and backup copies may be made if they would be useful when later restoring the files. Restoration proceeds by overwriting the frequently-changing files with stored copies and by undoing the changes to the logged files.

Data supplied from the **esp@cenet** database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2003-503793

(P2003-503793A)

(43) 公表日 平成15年1月28日 (2003.1.28)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 9/445		G 0 6 F 12/00	5 3 1 R 5 B 0 7 6
12/00	5 3 1	9/06	6 1 0 L 5 B 0 8 2

審査請求 未請求 予備審査請求 有 (全 28 頁)

(21) 出願番号 特願2001-507196(P2001-507196)
(86) (22) 出願日 平成12年6月30日 (2000.6.30)
(85) 翻訳文提出日 平成13年12月28日 (2001.12.28)
(86) 国際出願番号 PCT/US00/18324
(87) 国際公開番号 WO01/001252
(87) 国際公開日 平成13年1月4日 (2001.1.4)
(31) 優先権主張番号 60/141,757
(32) 優先日 平成11年6月30日 (1999.6.30)
(33) 優先権主張国 米国 (US)

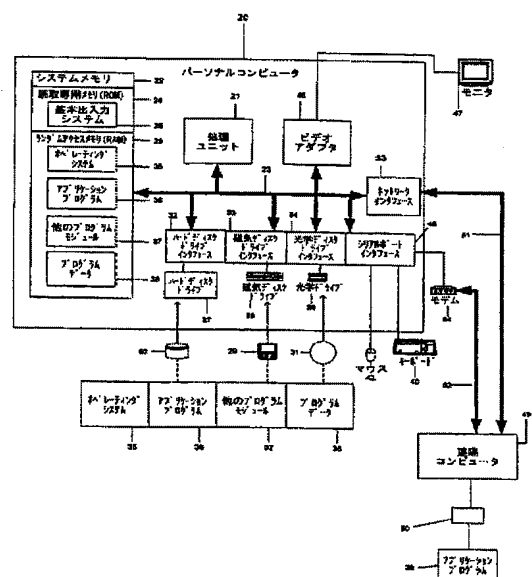
(71) 出願人 マイクロソフト コーポレイション
MICROSOFT CORPORATI
ON
アメリカ合衆国 ワシントン州 98052-
6399 レッドモンド ワン マイクロソフ
ト ウェイ (番地なし)
(72) 発明者 シッカ アシシュ
アメリカ合衆国 ワシントン州 98007
ベルビュー ワンハンドレッドアンドフォ
ーティーエイス アヴェニュー ノースイ
ースト #エム203 4385
(74) 代理人 弁理士 中村 稔 (外9名)

最終頁に続く

(54) 【発明の名称】 共用システムファイルを保護するシステム及び方法

(57) 【要約】

共用システムファイルを保護するシステム及び方法は、アプリケーションにより共用されるDLLファイルなどのシステムファイルがアプリケーションのインストール又は更新の間やユーザの行為によって無効なファイルで重ね書きされることを防ぐことによりシステムの安定性を高める。モニタリング構成要素は、システムファイルに対する変更を監視する。保護されたシステムファイルが変更されているのをモニタリング構成要素が検知した時、モニタリング構成要素は、オリジナルファイルのコピーを保存し、その変更をファイル保護サービスに報告する。ファイル保護サービスは、変更されたファイルを検査し、それが有効か否かを判断する。変更ファイルが無効である場合、システムファイルは、モニタリング構成要素が保存したコピーを用いてオリジナルの内容へ復元される。アプリケーション・インストーラ又は更新パッケージによるシステムファイルの未許可の持ち込みは、適切な権限を有する関係者が発行する証明書の使用を必要とすることにより防止される。



(2)

【特許請求の範囲】

【請求項1】 システムファイルに変更を行う呼び出しを監視する段階と、保護されるべき共用システムファイルに対して行なわれている変更を検知する段階と、

前記共用システムファイルに前記変更が為される前に、前記共用システムファイルのコピーを保存する段階と、

前記共用システムファイルに対する前記変更が有効であるか否かを判断する段階と、

前記変更が無効である場合、前記共用システムファイルの前記保存されたコピーを用いて前記変更を取り消す段階と、

を含むことを特徴とする、コンピュータシステムの共用システムファイルを保護する方法。

【請求項2】 請求項1に記載の方法を実行するコンピュータ実行可能命令を有することを特徴とする、コンピュータ読出可能媒体。

【請求項3】 前記共用システムファイルに対して為される前記変更は、前記共用システムファイルの異なるバージョンによる重ね書きであることを特徴とする請求項1に記載の方法。

【請求項4】 前記判断段階は、前記共用システムファイルの前記異なるバージョンのバージョン番号を前記コンピュータシステムにインストールされた前記共用システムファイルの最高バージョンと比較する段階を含むことを特徴とする請求項3に記載の方法。

【請求項5】 前記比較段階は、前記コンピュータシステムにインストールされた保護システムファイルを識別するデータを包含するデータベースから、前記共用システムファイルの前記最高バージョンに関するデータを検索する段階を含むことを特徴とする請求項4に記載の方法。

【請求項6】 前記判断段階は、前記異なるバージョンのハッシュ値を前記コンピュータシステムにインストールされた前記最高バージョンのハッシュ値と比較する段階を更に含むことを特徴とする請求項5に記載の方法。

【請求項7】 前記ハッシュ値の比較段階は、前記共用システムファイルに

(3)

関するインストールカタログの識別子を前記データベースから検索する段階と、前記コンピュータシステムにインストールされた前記最高バージョンの前記ハッシュ値を得るために前記インストールカタログにアクセスする段階とを含むことを特徴とする請求項6に記載の方法。

【請求項8】 請求項7に記載の方法を実行するコンピュータ実行可能命令を有することを特徴とする、コンピュータ読出可能媒体。

【請求項9】 前記取り消し段階は、前記異なるバージョンを前記共用システムファイルの前記保存コピーで重ね書きする段階を含むことを特徴とする請求項3に記載の方法。

【請求項10】 前記取り消し段階は、前記異なるバージョンを前記共用システムファイルの前記保存コピーで重ね書きするために、命令をシステム起動ファイルに挿入する段階を含むことを特徴とする請求項3に記載の方法。

【請求項11】 前記共用コンピュータファイルは、ダイナミック・リンク・ライブラリ（DLL）ファイルであることを特徴とする請求項1に記載の方法。

【請求項12】 前記検知段階は、変更されている前記共用システムファイルが保護されるべきか否かを判断するために、保護システムファイルのリストを参照する段階を含むことを特徴とする請求項1に記載の方法。

【請求項13】 更新パッケージを受け取る段階と、
前記更新パッケージの証明書を認証する段階と、
前記更新パッケージに含まれた共用システムファイルの更新バージョンを取り出す段階と、

前記コンピュータシステム上の前記共用システムファイルの現存バージョンを前記更新バージョンで重ね書きする段階と、

前記共用システムファイルの前記更新バージョンを含むために、前記コンピュータシステム上にインストールされた保護システムファイルを識別するデータベースを更新する段階と、

を更に含むことを特徴とする請求項1に記載の方法。

【請求項14】 請求項13に記載の方法を実行するコンピュータ実行可能

(4)

命令を有することを特徴とする、コンピュータ読出可能媒体。

【請求項15】 コンピュータシステムの共用システムファイルを保護するコンピュータ実行可能な構成要素であって、

モニタリング構成要素と、

ファイル保護サービス構成要素と、

を含み、

前記モニタリング構成要素は、システムファイルに対する変更を監視し、保護共用システムファイルに対して為されている変更を検知すると前記変更が為される前に前記保護共用システムファイルのコピーを保存し、前記ファイル保護サービス構成要素に通知し、前記サービス構成要素は、前記通知に応答して前記変更が有効か否かを判断し、前記変更が有効でない場合には前記保護共用システムファイルの前記保存コピーを用いて前記変更を取り消す、ことを特徴とする構成要素を有するコンピュータ読出可能媒体。

【請求項16】 前記モニタリング構成要素は、システムファイルを変更するためのファイルシステムドライバへの呼出しを監視するために前記ファイルシステムドライバの上に置かれることを特徴とする請求項15に記載のコンピュータ読出可能媒体。

【請求項17】 前記共用システムファイルに対する前記変更は、前記共用システムファイルの異なるバージョンによる重ね書きであることを特徴とする請求項15に記載のコンピュータ読出可能媒体。

【請求項18】 前記ファイル保護サービス構成要素は、前記コンピュータシステム上にインストールされた保護システムファイルを識別するインストールされたファイルのデータベースを保持し、前記共用システムファイルの前記異なるバージョンが有効か否かを判断する際に前記インストールファイル・データベースを参照することを特徴とする請求項15に記載のコンピュータ読出可能媒体。

【請求項19】 前記インストールファイル・データベースは、前記コンピュータシステム上にインストールされた前記保護システムファイルの各々に対するインストールされた最高バージョンとハッシュ値とを識別し、前記ファイル保

(5)

護サービス構成要素は、変更されている前記保護システムファイルの前記インストールされた最高バージョンとハッシュ値とを前記異なるバージョンが有効か否かを判断するために使用することを特徴とする請求項18に記載のコンピュータ読出可能媒体。

【請求項20】 前記ファイル保護サービス構成要素は、保護ファイルリストを更に保持し、前記モニタリング構成要素は、前記変更が前記保護共用システムファイルに対して為されているのを検知すると前記保護ファイルリストにある前記保護共用システムファイルを識別することを特徴とする請求項19に記載のコンピュータ読出可能媒体。

【請求項21】 前記ファイル保護サービス構成要素は、
更新パッケージを受け取る段階と、
前記更新パッケージを認証する段階と、
前記更新パッケージに含まれた共用システムファイルの更新バージョンを取り出す段階と、
前記コンピュータシステム上の前記共用システムファイルの現存バージョンを前記更新バージョンで重ね書きする段階と、
前記共用システムファイルの前記更新バージョンを含むために、前記インストールファイル・データベースを更新する段階と、
を実行するように更にプログラムされることを特徴とする請求項20に記載のコンピュータ読出可能媒体。

【請求項22】 前記保護共用システムファイルは、ダイナミック・リンク・ライブラリ(DLL)ファイルであることを特徴とする請求項15に記載のコンピュータ読出可能媒体。

(6)

【発明の詳細な説明】

【0001】

(技術分野)

本発明は、一般的にコンピュータオペレーティングシステムに関し、更に特定すれば、異なるアプリケーションが共用する重要なオペレーティングシステムファイルの保護に関する。

【0002】

(背景技術)

今日のコンピュータオペレーティングシステムは、その構成に多くの層を有する場合があり、異なる機能を果たすために無数のファイルを含んだ高度に複雑なプログラムである。オペレーティングシステム（オペレーティングシステム）の構成要素の幾つかは、システムにインストールされたアプリケーションに様々なシステム機能を準備するように設計されており、従って、アプリケーションによって「共用」される。例えば、マイクロソフト・コーポレーションのWINDOWS（登録商標）オペレーティングシステムには、アプリケーションプログラムが実行時にリンクしてそこに実装された機能を呼び出すことができる多くのファイルがダイナミック・リンク・ライブラリ（DLL）ファイルの形で存在する。

【0003】

DLLファイルなどの共用オペレーティングシステムファイルは、多数の異なるアプリケーションによって使用されるから、それらの共用システムファイルのうちの1つが変造されたり、不用意に重ね書きされたり、又は、他の方法で破壊されると、多くの数のアプリケーションが働きを停止する場合がある。従って、共用システムファイルに対する無効な変更は、システム不安定の重大な原因となる可能性がある。例えば、WINDOWS（登録商標）オペレーティングシステムは、第三者のアプリケーションのインストーラプログラムがこのアプリケーションによって必要とされる全てのファイルをこのアプリケーションのインストール中にシステムに加えることを許している。インストール中に加えられたそれらのファイルは、他のアプリケーションにより共用されるDLLファイルを含むことがしばしばである。インストーラは、システムファイルを変更す

(7)

るその能力により、アプリケーションが設計通りに実行されるために必要な全てのファイルを有することになるのを確実にすることができる。しかし、このことは、他のアプリケーションが必要とする共用システムファイルに対してインストーラが不適切な変更を同じく加えることができるので、オペレーティングシステムをシステム不安定という重大な問題にも直面させる。例えば、より古いアプリケーションのインストーラは、システム上の既存のDLLファイルを、より新しいアプリケーションとは一緒に働かないそのファイルのより古いバージョンで重ね書きする場合がある。ソフトウェア専門業者の中には、DLLファイルの他のアプリケーションと互換性のないいくつかの専売権付きバージョンで選ばれたDLLファイルを重ね書きすることを試みるものもある。オペレーティングシステムが更に複雑化し、益々多くのアプリケーションが入手可能になるにつれて、アプリケーションのインストール又は更新の間に共用システムファイルが無効バージョンで重ね書きされる危険性が益々増大している。共用オペレーティングシステムファイルの不適切な変更起因するシステムの不安定性は、最近ではユーザが体験する非常に重大な問題となっており、オペレーティングシステムを比較する際の重要な要素となっている。

【0004】

(発明の開示)

上記の観点から、本発明は、共用システムファイルを保護するシステム及び方法を提供し、それは、アプリケーションのインストール又は更新中、又は、ユーザの行為により、アプリケーションによって共用されるDLLファイルなどのシステムファイルが不適切に変更されないように保護をする。共用システムファイルを保護するために、オペレーティングシステムには、システムファイルの変更を監視するモニタリング構成要素が備えられる。保護されたシステムファイルが変更されている時、モニタリング構成要素は、オリジナルファイルのコピーを記憶し、その変更についてシステムファイル保護(SFP)サービスに報告する。SFPサービスは、変更ファイルを検査して、そのファイルが有効か否かを判断する。変更ファイルが無効であれば、システムファイルは、モニタリング構成要素により記憶されたコピーを用いてそのオリジナルの内容に復元される。アプリ

(8)

ケーション・インストーラ又は更新パッケージによるシステムファイルの未許可の持ち込みは、そのシステムファイルがインストールされることを表すそのパッケージに関する有効な証明書を要求することにより同じく防止される。

本発明の更なる形態や利点は、添付図面の参照と共に進められる例証的な実施形態に関する以下の詳細な説明から明らかになるであろう。

添付請求項は、本発明の形態を詳細に列挙するが、その目的及び利点と共に本発明は、添付図面に関連して為される以下の詳細な説明によって最も良く理解することができる。

【0005】

(発明を実施するための最良の形態)

同様な参照番号が同様な部材を示す添付図面を参照すると、本発明は、適切な計算環境に実装された状態で示されている。必ずしもそれに限定されないが、本発明は、パーソナルコンピュータによって実行される、プログラムモジュールなどのコンピュータ実行可能命令との一般的な関連において以下に記述される。一般にプログラムモジュールは、特定のタスクを実行するか、又は、特定の抽象的データタイプを実装する、ルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。更に、手持式装置、マルチプロセッサシステム、マイクロプロセッサ式又はプログラム可能な消費者向け電子機器、ネットワーク・パーソナルコンピュータ、ミニコンピュータ、及び、メインフレームコンピュータなどを含む、他のコンピュータシステム形態を用いて本発明を実施してもよいことを当業者は理解するであろう。本発明はまた、タスクが通信ネットワークを通じて接続された遠隔処理装置によって実行される分散型計算環境において実施してもよい。分散型計算環境においては、プログラムモジュールは、ローカル及び遠隔記憶装置の両方に置くことができる。

【0006】

図1を参照すると、本発明を実装する例示的システムは、汎用計算装置を従来のパーソナルコンピュータ20の形で含んでおり、この汎用計算装置は、処理ユニット21、システムメモリ22、及び、システムメモリを含む様々なシステム構成要素を処理ユニット21に結合するシステムバス23を含む。システムバス

(9)

23は、メモリバス又はメモリ制御装置、周辺バス、及び、様々なバス構造のいずれかを用いるローカルバスを含む幾つかの種類のバス構造のいずれでもよい。

システムメモリは、読取り専用メモリ (ROM) 24とランダムアクセスメモリ (RAM) 25とを含む。起動時などにパーソナルコンピュータ20における素子間の情報転送を補助する基本ルーチンを包含する基本入出力システム (BIOS) 26は、ROM24に記憶される。パーソナルコンピュータ20は、ハードディスク60に対して読出し及び書込みを行うハードディスクドライブ27、取外し可能磁気ディスク29に対して読出し又は書込みを行う磁気ディスクドライブ28、及び、コンパクト・ディスク・ROMや他の光学的手段などの取外し可能光学ディスク31に対して読出し又は書込みを行う光学ディスクドライブ30を更に含む。

【0007】

ハードディスクドライブ27、磁気ディスクドライブ28、及び、光学ディスクドライブ30は、各々、ハードディスクドライブインタフェース32、磁気ディスクドライブインタフェース33、及び、光学ディスクドライブインタフェース34により、システムバス23に接続されている。これらのドライブとそれらに付随するコンピュータ読取可能手段は、コンピュータ読取可能命令、データ構造、プログラムモジュール、及び、パーソナルコンピュータ20のための他のデータの不揮発性記憶装置を準備する。本明細書で説明する例示的環境は、ハードディスク60、取外し可能磁気ディスク29、及び、取外し可能光学ディスク31を採用するが、磁気カセット、フラッシュメモリカード、デジタルビデオディスク、ベルヌーイカートリッジ、ランダムアクセスメモリ、及び、読取り専用メモリなど、データを記憶できるコンピュータでアクセス可能な他の種類のコンピュータ読取可能手段を例示的作動環境で同じく使用してもよいことは当業者により理解されるであろう。

【0008】

オペレーティングシステム35、1つ又はそれ以上のアプリケーションプログラム36、他のプログラムモジュール37、及び、プログラムデータ38を含むいくつかのプログラムモジュールは、ハードディスク60、磁気ディスク29、

(10)

光学ディスク31、ROM24、又は、RAM25上に記憶してもよい。ユーザは、キーボード40や指示装置42などの入力装置を通じてパーソナルコンピュータ20の中に指令及び情報を入力することができる。他の入力装置（図示しない）には、マイクロホン、操作棒、ゲームパッド、衛星用ディッシュ、及び、走査器などが含まれてもよい。これら及び他の入力装置は、システムバスに結合されたシリアルポートインタフェース46を通じて処理ユニット21に接続されることが多いが、パラレルポート、ゲームポート、又は、ユニバーサルシリアルバス（USB）などの他のインタフェースによって接続されてもよい。モニタ47又は他の種類の表示装置は、ビデオアダプタ48などのインタフェースを通じて同じくシステムバス23に接続される。モニタに加えてパーソナルコンピュータは、一般的にスピーカやプリンタなどの図示しないが他の周辺出力装置を含む。

【0009】

パーソナルコンピュータ20は、遠隔コンピュータ49などの1つ又はそれ以上の遠隔コンピュータへの論理結合を用いるネットワーク環境で作動してもよい。遠隔コンピュータ49は、別のパーソナルコンピュータ、サーバ、ルータ、ネットワークパーソナルコンピュータ、ピア装置、又は、他の普通のネットワークノードであってもよく、図1にはただ記憶装置50のみが示されているが、通常、パーソナルコンピュータ20に関して上記で説明した構成品の多く又は全てを含む。図1に示された論理結合は、ローカルエリアネットワーク（LAN）51とワイドエリアネットワーク（WAN）52とを含む。そのようなネットワーク環境は、事務所、企業間コンピュータネットワーク、イントラネット、及び、インターネットにおいてありふれたものである。

【0010】

LANのネットワーク環境で使用される場合、パーソナルコンピュータ20は、ネットワークインタフェース又はアダプタ53を通じてローカルネットワーク51に接続される。WANのネットワーク環境で使用される場合、パーソナルコンピュータ20は、一般的には、WAN52上の通信を確立するためにモデム54又は他の手段を含む。内臓モデム又は外付けモデムであり得るモデム54は、シリアルポートインタフェース46を通じてシステムバス23に接続される。ネ

(11)

ットワーク環境においては、パーソナルコンピュータ20又はその一部分に対して書かれたプログラムモジュールは、遠隔記憶装置に記憶することができる。図示のネットワーク接続は例証的であり、コンピュータ間の通信リンクを確立する他の手段を使用してもよいことが理解されるであろう。

【0011】

以下の記述において、特に断らない限り、本発明は、1つ又はそれ以上のコンピュータによって実行される作用か、又は、作動の記号的表示かに関連して説明される。従って、時には「コンピュータで実行された」として言及されるそのような作用又は作動は、データの構造化された形態を表す電気信号をコンピュータの処理ユニットが操作することを含むことが理解されるであろう。この操作は、データを変換するか、又は、当業者にはよく理解されている方法でコンピュータの作動を再構成又はそうでなければ変更するコンピュータのメモリシステムの各位置にデータを保持する。データが維持されるデータ構造は、データ書式により規定される特質を有するメモリの物理的位置である。しかし、本発明は上記の関連で記述されているが、当業者が理解するように、それは限定的であることを意味せず、以下に述べる様々な作用及び作動は、ハードウェアに実装されてもよい。

【0012】

ここで図2を参照すると、本発明は、DLLファイルなどの共用システムファイルを不注意で無効バージョンにより重ね書きされたり、又は、他の方法で不適当に変更されることから保護する効果的な方法に関する。以下に説明する好ましい実施形態において、オペレーティングシステムは、マイクロソフト・コーポレーションのWINDOWS（登録商標）オペレーティングシステムであってもよく、アプリケーションによって共用され、保護されるシステムファイルの一例として、DLLファイルが使用される。しかし、本発明によるシステムファイル保護は、共用システムファイルを有する他のオペレーティングシステムと共に使用されるほか、他の種類の共用システムファイルを保護するためにも使用できるということが理解されるであろう。

【0013】

(12)

図2に示すように、オペレーティングシステム70は、実行中に様々なシステム機能を提供するために呼び出されてアプリケーション74に動的に接続することができる複数のダイナミックリンクライブラリ(DLL)ファイル72を有する。DLLファイルに関しては、高められた機能をもたらすため又はバグを取り除くために過去に何度も更新されていることは普通のことであるから、与えられたDLLファイルの幾つかの異なるバージョンが存在する場合がある。DLLファイルの異なるバージョンを憶えておくために、図示の実施形態における各DLLファイルは、その名前によって識別されるだけでなく、付随するバージョン番号によっても識別される。

【0014】

上記の通り、システム不安定性の1つの主要原因は、アプリケーションのインストール又は更新パッケージ66のインストーラが現存の共用システムファイルを他のアプリケーションと共に実行できないバージョンで重ね書きすることを試みる場合があるということである。例えば、より古いアプリケーションは、より古いバージョンでDLLファイルの重ね書きを試みる場合があり、又は、あるアプリケーションは、他のアプリケーションと適合しない専売権付きバージョンでDLLファイルの重ね書きを試みる場合もある。アプリケーションのインストール又は更新は、共用システムファイルが不適切に重ね書きされたり、又は、他の方法で変造や破壊される筋書きの1つであるに過ぎないことが理解されるであろう。例えば、共用システムファイルは、ユーザ68の行為により不適切に変更されたり、削除されたりすることもある。以下の記述の観点から明らかになるように、本発明によるシステムファイル保護は、そのようなユーザの行為に対しても、また同様に、保護されたシステムファイルを未許可に変更する他の原因に対しても同じく有効である。

【0015】

本発明によれば、共用システムファイルの保護は、2つの関連する態様において実行される。第1に、すでにシステムに存在するシステムファイルは、無効なファイルで重ね書きされることから保護される。この目的のために、システムファイルの変更が監視される。保護されたシステムファイルが無効なファイルで重

(13)

ね書きされるか又は他の方法で不適切に変更されると、この無効な変更が検知されて取り消され、オリジナルファイルを復元する。第2に、アプリケーションのインストレーション又は更新中におけるシステムファイルの未許可の持ち込みは許可されず、システムに無効なシステムファイルが追加されるのを防ぐ。

【0016】

第1の態様に戻ると、図示の実施形態において、未許可の変更からの現存システムファイルの保護は、ファイル変更モニタリング構成要素とシステムファイル保護(SFP)サービス構成要素80との協働によって達成される。図示の実施形態において仮想デバイスドライバ(Vxd)82として示されているモニタリング構成要素は、保護システムファイルの変更を監視し、この変更をSFPサービス80に告げる責任がある。これらが無効な変更であると判断された場合、SFPサービス80は、この変更を取り消すことができる。図2に示すように、オペレーティングシステム70のファイルシステムマネージャ86とファイルシステムドライバ88との間には、モニタリング構成要素(Vxd)82が挿入されている。Vxd82をこの位置に有することにより、システムメモリ90に記憶されたファイルに対する作動のためのシステムファイルマネージャ86からシステムファイルドライバ88への全ての呼び出しは、Vxdを通過することになる。このようにして、Vxd82は、システムファイルのあらゆる変更を追跡することができる。ファイルの変更としては、ファイルを別のファイルで重ね書きすること、ファイルのいくつかのデータを変更すること、又は、ファイルを削除することに関わる場合がある。

【0017】

Vxd82がファイルを変更する呼び出しを受け取った時、Vxd82は、そのファイルについて責任のあるファイルシステムドライバ88に向けてその呼び出しを直ちには転送しない。その代わりに、Vxdは、最初に保護システムファイルのリスト92を検査し、変更されるこのファイルが本実施形態においてはDLLファイルを含む保護システムファイルのうちの1つであるか否かを調べる。そのファイルが保護システムファイルである場合、Vxd82は、最初にオリジナルファイルのコピーを作成し、変更が為されるのを許可する前に、このコピー

(14)

をシステムの一時的ディレクトリ96に記憶する。次いで、Vxd82は、SFPサービス80に対して保護ファイルが変更されたことを報告する。図示の実施形態においては、Vxd82とSFPサービス80との間の通信は、WINDOWS（登録商標）のメッセージによるものであり、SFPサービスは、メッセージループで実行されている。

【0018】

一例として、図2に示すように、変更されるシステムファイルは、バージョン番号2を有する「abc. d11」と名付けられたファイルであってもよい。このファイルをabc. d11のバージョン1で重ね書きするという呼び出しを受け取った時、Vxd82は、保護ファイルのリスト92を検査してこのファイルが保護されるべきであると判断する。次に、Vxd82は、abc. d11のv2（バージョン2）のコピーを一時的ディレクトリ96に記憶する。システムメモリ90のファイルabc. d11のv2は、次に、abc. d11のv1（バージョン1）で置き換えられる。

【0019】

SFPサービス80は、Vxd82から保護システムファイルが変更されたとの報告を受け取ると、その変更が許されるか否かを検査する。オリジナルファイルが新しいファイルで重ね書きされる場合、SFPサービスは、新しいファイルが有効か否かを判断する。新しいファイルが無効である場合、SFPサービス80は、Vxd82によって一時的ディレクトリに記憶されたオリジナルファイルのコピーでこの新しいファイルを置き換え、それによってその変更を取り消す。

【0020】

いくつかの場合には、保護ファイルに対する意図された変更は直ちには実行されないで、後で実行すべく延期される。例えば、共用システムファイルが連続的に使用されており、それへの書き込み作動が実行できない場合には、ファイルシステムマネージャは、目標のシステムファイルを新しいファイルで重ね書きする書込命令100をシステム起動ファイル98に置くように決めることができる。システムが次回に起動されると、システム起動ファイルの書込命令が実行されることになり、変更が達成される。この筋書きの場合、新しいファイルが無効であ

(15)

るとSFPサービス80が判断した場合、SFPサービス80は、単に書込命令100をシステム起動ファイルから除去するだけであり、これによって無効な変更が起こるのを防止する。

【0021】

これと関連する筋書きにおいて、SFPサービス80が新しいファイルは無効であると判断したが、アプリケーションによるこのシステムファイルの連続使用がSFPサービス80によるオリジナルファイルの復元を制限する時、オリジナルシステムファイルの無効なバージョンによる重ね書きが既に起こっている場合がある。この場合には、Vxd82により保存されたオリジナルファイルのコピーで変更されたシステムファイルを重ね書きするために、SFPサービス80は、書込命令102をシステム起動ファイル98に置くように決めることができる。すなわち、次のシステム起動中に、システムファイルはそのオリジナルの形に復元されることになる。

【0022】

ある実施形態においては、Vxd82により検査される保護システムファイルのリスト92は、拡張可能なマークアップ言語（XML）書式でファイルに含まれる。説明の便宜上、図3は、そのようなXMLファイルの単純化された例を示している。この例において、XMLファイル106は、他のシステム管理目的のためにファイルを識別するためにも使用される。保護される共用システムファイルは、段落108において「SEP」タグを用いて識別される。図を単純化するために、図3に示すXMLファイル106の「SFP」段落は、2つのエントリのみを含む。しかし、実際の実行に際しては、保護されたシステムディレクトリやファイルを識別するために、この段落には多くのエントリがあってもよいことが理解されるであろう。この実施形態においては、この「SFP」段落の各ステートメントは、保護されるシステムファイル（それが入っているディレクトリを含む）を識別する。XMLファイルは、オペレーティングシステムを備えており、ファイルをリストに加えたり、又は、リストから除去する必要がある時には、更新パッケージを用いて更新することができる。システムファイルが書込演算のために開かれている時、Vxd82は、XMLファイルを検査し、システムファ

イルがXMLファイルの「SFP」段落に現れているか否かを調べる。もし現れていれば、システムファイルは保護されることになり、Vxdは、そのシステムファイルがいかなる変更を受けるよりも前にそのコピーを作成する。

【0023】

変更システムファイルが有効か否かをSFPサービス80が判断できるようにするために、SFPサービスは、システム上にインストールされた共用システムファイルを識別するシステムファイル保護(SFP)データベース110を保持する。説明の便宜上、図4にSFPデータベース110の例を表の形式で示す。システムファイルの持ち込み制御と関連して一層詳細に後述するように、アプリケーション・インストーラ又は更新パッケージによって加えられるシステムファイルは、オペレーティングシステムに呈示される1つ又はそれ以上のカタログで識別されるのが好ましい。図4に示すように、SFPデータベース110の各エントリは、保護されたDLLファイルの名称とそのファイルが提示されたカタログのほか、そのカタログで特定されたそのファイルのバージョン番号を記憶する。ある与えられたファイル名が多くのカタログに列挙されている場合、同一ファイル名を有する多くのエントリが存在してもよい。ただし、同一ファイル名を有するエントリの各々は、異なるバージョン番号及び／又はそれに付随するカタログ名を有することになるであろう。例えば、図4に示す例においては、Winsock.dllに対して2つのエントリが存在しており、それらは、各々、カタログのMill.catとMillSP1.catとに付随し、バージョン番号の6.0と7.0とを有する。

【0024】

好ましい実施形態の態様によれば、保護システムファイルは、そのファイル名とバージョン番号とによってのみならず、ハッシュ値によっても識別される。ある与えられたファイルのハッシュ値は、ハッシュ関数をファイルの内容に適用することによって作り出される。ハッシュ関数とは、ファイルにおける1つのビットの変更さえも異なるハッシュ値をもたらす可能性が高くなるといったようなものである。同時に、ハッシュ値から逆にファイルの内容を引き出すことはできない。後述するように、保護システムファイルをそのハッシュ値で識別することは

(17)

、そのファイル名とバージョン番号とが同じままであるにもかかわらず、その内容が変更されたか否かの判断を可能にする。好ましい実施形態においては、保護システムファイルのハッシュ値は、そのファイルをシステム上にインストールするために使用された対応するカタログに記憶され、カタログは、システムのカタログ記憶装置140（図5）に保持される。

【0025】

保護システムファイルが変更されたというVxd82からのメッセージをSFPサービス80が受け取った時、SFPサービスは、SFPデータベース110に対して、変更されたものと同じファイル名を有するデータベース内の全てのエントリを問い合わせる。次に、SFPサービスは、データベースからの情報に基づいて、その「新しいファイル」が有効か否かを判断する。新しいファイルは、

（1）新しいファイルがSFPデータベースのそのファイルに対するエントリの最高バージョン番号と同じバージョン番号を有し、（2）新しいファイルがそのバージョン番号に対する正しいハッシュ値を有する場合、それは有効と見なされる。この2番目の比較に関して、SFPサービス80は、SFPデータベースエントリの最高バージョン番号を読み取ってこれに付随するカタログを識別し、そのバージョンに対するハッシュ値を得るためにカタログ記憶装置140のそのカタログを読み出す。新しいファイルが正しいハッシュ値を持つことを必要とすることは、オリジナルファイルが同じファイル名と正しいバージョン番号とを有するが変更されて無効な内容を有するファイルで重ね書きされる危険性を防止する。

【0026】

ここで、本発明によるファイル保護の第2の態様に戻ると、システムファイルの持ち込みは綿密に監視され、それらが適正な許可の表示を伴っている場合にのみシステムに加えることが許可される。好ましい実施形態においては、システムファイルの持ち込みは、アプリケーション・インストール又はアプリケーション更新パッケージのいずれかによって行うことができる。いずれの場合にも、システムに置かれるシステムファイルは、カタログに提示される。カタログで識別されたシステムファイルをインストールする演算は、アプリケーションをイ

インストールする場合と更新パッケージをインストールする場合の両方で同じであるから、以下では更新パッケージをインストールする場合についてのみ記述される。この観点から言えば、アプリケーション・インストール・パッケージは更新パッケージの一種であると思ってもよいことが理解されるであろう。

【0027】

図5は、説明のためにカタログ120の例を示す。カタログは多重エントリを有してもよく、各エントリは、システムに加えられるシステムファイルを識別する。エントリは、例えば、ファイル名、そのファイルのハッシュ値、及び、ファイルのバージョン番号を準備する。エントリは、ファイルに関する他のデータを同じく含んでもよい。図示の実施形態においては、カタログは、システムにインストールされる更新パッケージ122の一部である。

【0028】

無効なファイルがシステムに持ち込まれて共用システムファイルを重ね書きするために使用されるのを防ぐために、更新パッケージ122には、そのカタログ及び付随するファイル126が受け入れられることになる前に適正な許可を示すことが要求される。好ましい実施形態においては、この許可検査は、更新パッケージ122と共に含まれる証明書128によって行なわれる。この証明書128は、パッケージの真正性と完全性を保証する良く知られた証明書型認証技術に従って適切な証明書機関132によって発行することができる。証明書を発行する証明書機関132は、例えば、オペレーティングシステムの製造会社であってもよいし、又は、正しく作られたインストール又は更新パッケージを証明する責任を委託されたいかなる他の関係者であってもよい。保護システムファイルのいかなるインストールも有効な証明書を伴うことが必要であることにより、その証明書を発行する機関132は、パッケージに呈示された全てのシステムファイルが有効であることを検査することができる。

【0029】

一般に、更新パッケージ122は、インストーラ136、1つ又はそれ以上のカタログ120、及び、システムに加えられる全てのシステムファイル及びアプリケーションファイル126を包含する圧縮キャビネット(CAB)ファイル1

24の形態を有する。オペレーティングシステムがCABファイルを用いて提示された時、オペレーティングシステムは、最初に、パッケージに含まれている証明書128が適切な機関によって発行されたか否かを検査する。適切な機関によって発行されている場合は、ファイルの完全性、すなわちファイルが変更されたことがないことを証明するために証明書が用いられる。証明書を認証した後、CABファイル内に圧縮されたファイルが取り出される。パッケージ内のインストーラ136は、上記の通り、次にカタログとカタログに列挙されたファイルとをインストールすることを許される。

【0030】

カタログ120で識別されたシステムファイルをインストールするために、更新パッケージ122のシステム構成要素インストーラ136は、オペレーティングシステムのカタログ・アプリケーションプログラミングインタフェース(API)138を呼び出す。カタログAPI138は、インストールカタログ(InstallCatalog)機能とアンインストールカタログ(UninstallCatalog)機能とを呈示する。カタログ120で識別されたシステムファイルをインストールするために、インストーラ136は、インストールカタログ機能と呼び出してカタログを提示する。これに呼応して、SFPサービス80は、カタログ120のエントリを列挙してこれらを上記の通りSFPデータベースに加え、システムファイルをそれらの適正ディレクトリにコピーする。カタログ120は、カタログ記憶装置140にも加えられる。その後、SFPデータベース110がいくらか変造された場合、システムにインストールされた保護システムファイルを特定するためにカタログ記憶装置140の全てのカタログを列挙することにより、SFPデータベースを再構築することができる。

更新パッケージのインストーラがカタログの除去を欲する時、インストーラは、カタログAPI138のアンインストールカタログ機能と呼び出す。このアンインストール要求に応答して、SFPサービス80は、SFPデータベース110に対してデータベースにあるその与えられたカタログに付随する全てのエントリについて問い合わせ、それらのエントリをデータベースから除去する。

【0031】

(20)

本発明の原理を適用し得る多くの可能な実施形態の観点において、図面の各図に関連して本明細書で記述した実施形態は単に例証的であることを意味しており、本発明の範囲を限定するように解釈してはならないことを理解されたい。例えば、ソフトウェアの形で示され説明された実施形態の要素をハードウェアに実装してもよいしその逆もまた可能であり、あるいは、説明された実施形態が本発明の精神から逸脱することなく構成や細部を変更できることを当業者は理解するであろう。従って、本明細書で記述された本発明は、そのような全ての実施形態が添付請求項及びその同等形態の範囲に該当するように意図されている。

【図面の簡単な説明】

【図1】

本発明が適用される例示的コンピュータシステムを一般的に示すブロック図である。

【図2】

共用システムファイルを保護する本発明による構成要素を有するオペレーティングシステムの実施形態を示す概略図である。

【図3】

保護されるシステムファイルを識別する図2の実施形態で使用される例示的XMLファイルを示す図である。

【図4】

保護システムファイルに関する情報を提供するシステムファイル保護（SFP）データベースにおけるデータ構造の概略図である。

【図5】

有効な証明書の提示に基づくインストレーション／更新パッケージにより与えられるシステムファイルの制御された持ち込みを示す概略図である。

(21)

【図 1】

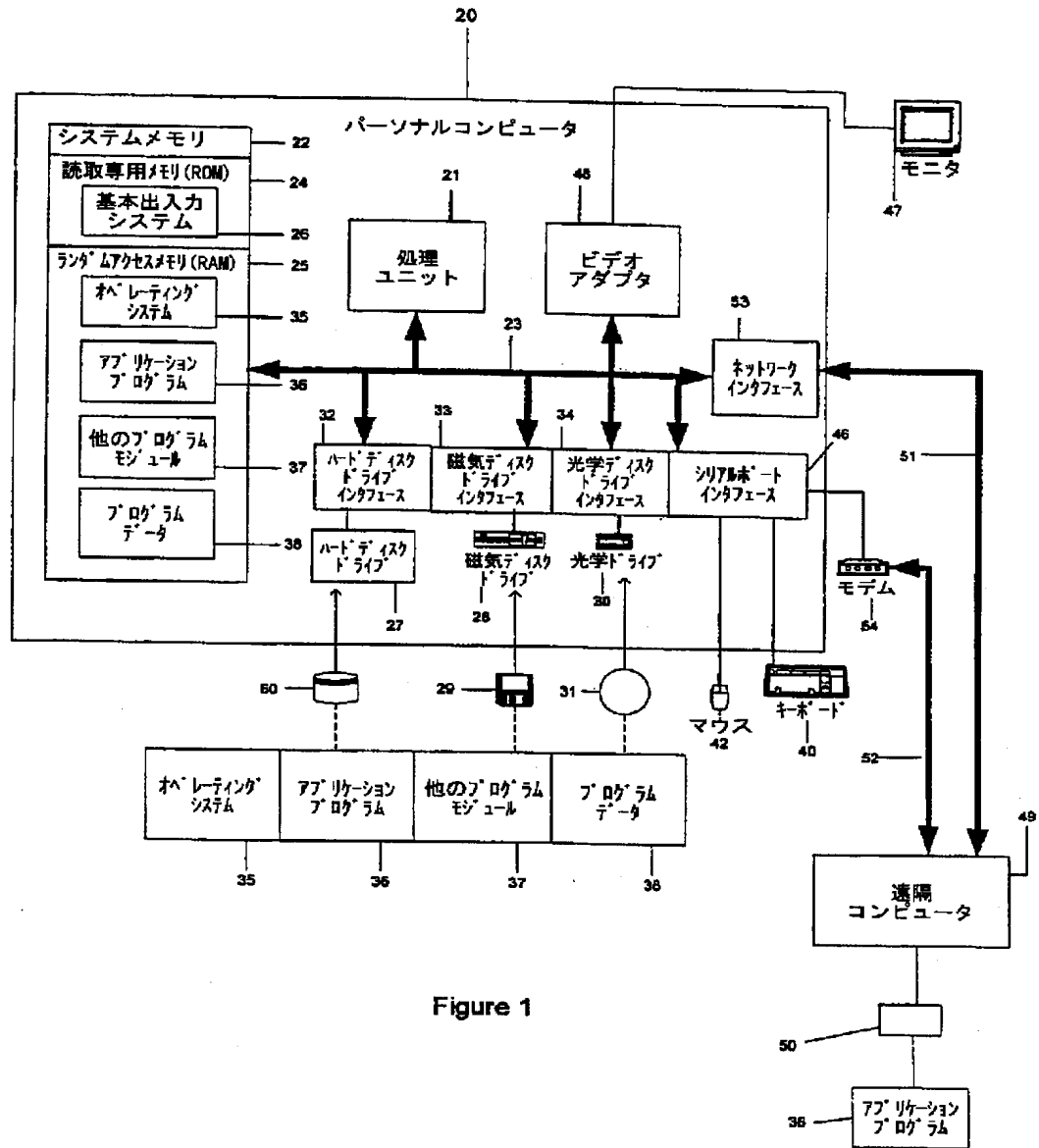


Figure 1

(22)

【図2】

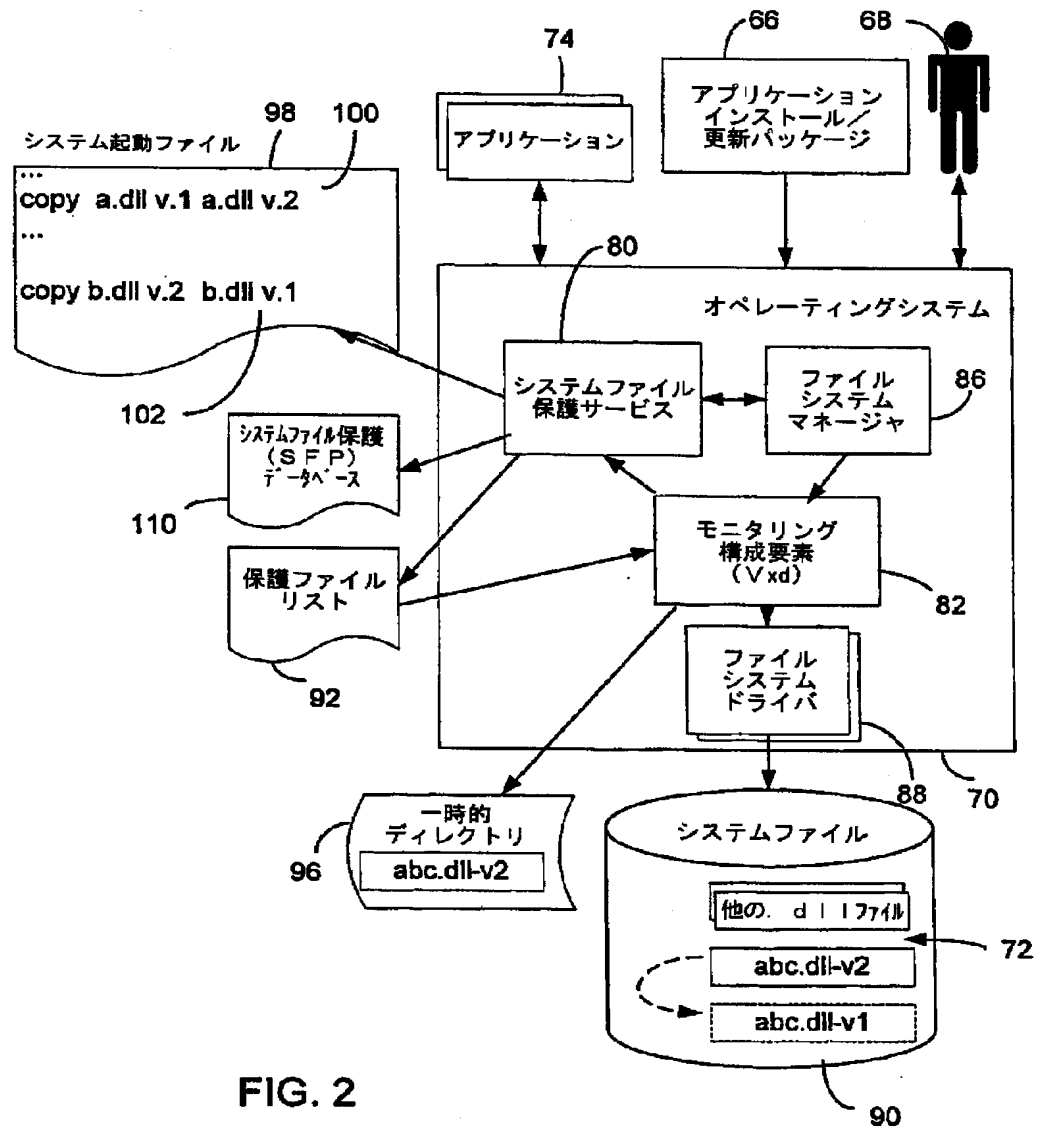


FIG. 2

(23)

【図 3】

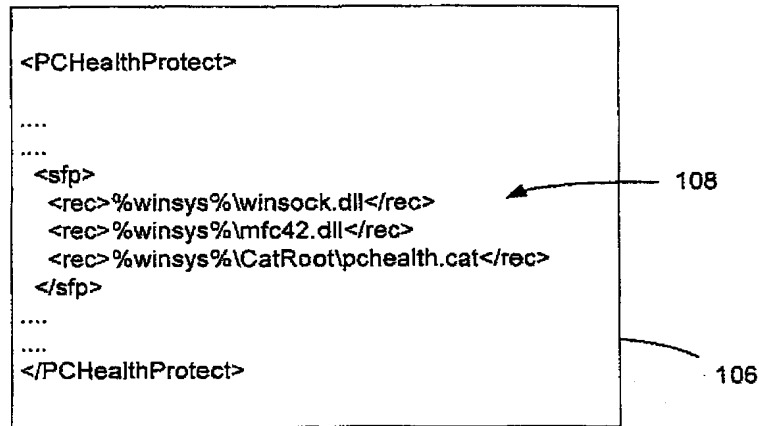


FIG. 3

【図 4】

FIG. 4

110

システムファイル保護 (SFP) データベース

ファイル名	カタログ	バージョン
Winsock.dll	Mill.cat	6.0
Winsock.dll	MillSP1.cat	7.0
Msvcrt.dll	MillSP1.cat	9.0
Oleaut32.dll	Mill.cat	6.0

(24)

【図 5】

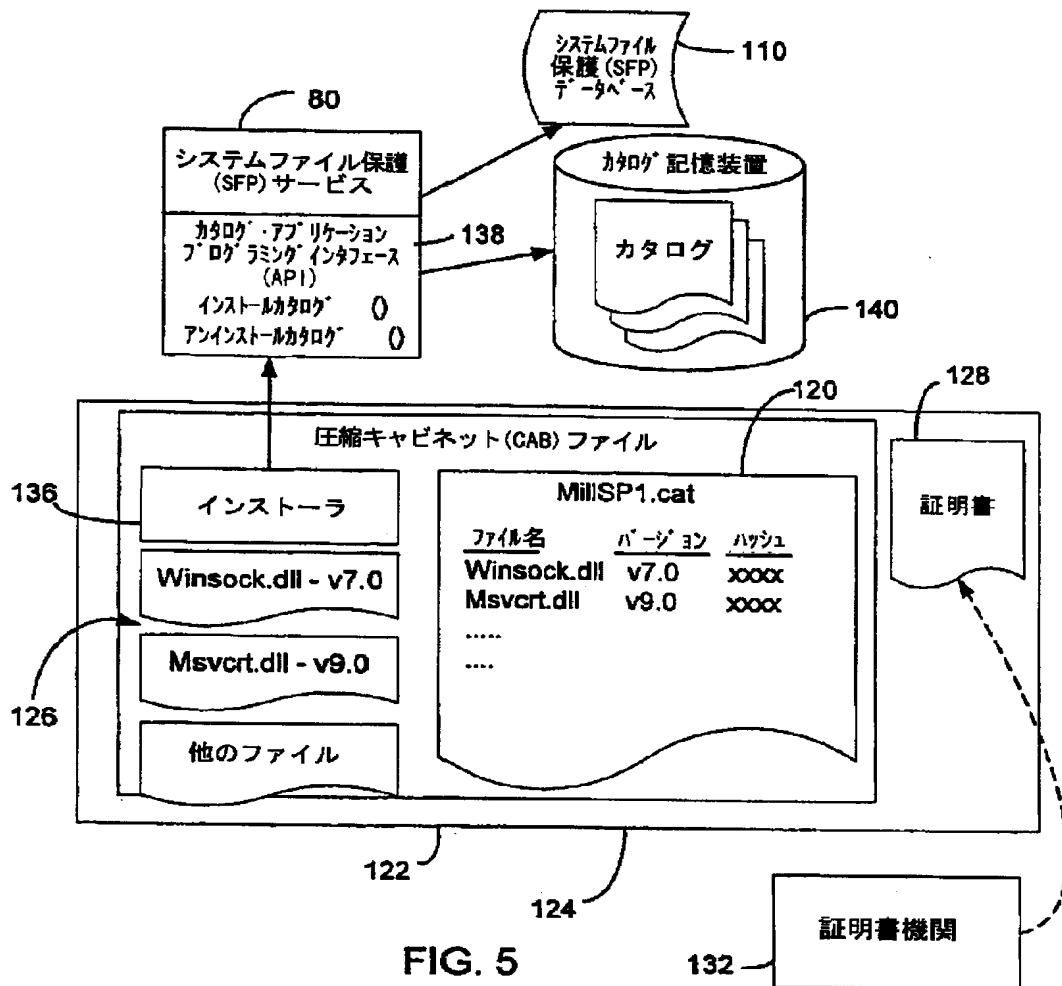


FIG. 5

(25)

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US 00/18324A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F11/14 G06F9/44

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"SAFE INSTALLATION OF OBJECT-ORIENTED CLASS LIBRARIES COMMON TO MULTIPLE SOFTWARE PRODUCTS" IBM TECHNICAL DISCLOSURE BULLETIN, US, IBM CORP. NEW YORK, vol. 37, no. 28, 1 February 1994 (1994-02-01), pages 407-409, XP000433893 ISSN: 0018-8689 * the whole document *	1-3, 9, 11-13, 15, 22
A	US 5 715 462 A (BRYEN MARK D ET AL) 3 February 1998 (1998-02-03) column 3, line 43 - column 6, line 9; claims 1, 2	13-17
	---	---

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents:

- * "A" document defining the general state of the art which is not considered to be of particular relevance
- * "E" earlier document but published on or after the international filing date
- * "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- * "O" document referring to an oral disclosure, use, exhibition or other means
- * "P" document published prior to the international filing date but later than the priority date claimed

- * "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- * "X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- * "Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- * "Z" document member of the same patent family

Date of the actual completion of the international search

4 December 2000

Date of mailing of the international search report

11/12/2000

Name and mailing address of the ISA

European Patent Office, P.O. 5010 Patentean 2
NL - 2280 HV Rijswijk
Tel: (+31-70) 340-2040, TX: 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Fransen, L

Form PCT/ISA/210 (second sheet) (July 1992)

(26)

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US 00/18324

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	COLLINSON: "Putting old software back together again" EXE , vol. 13, no. 6, November 1998 (1998-11), pages 45-48, XP000965369 UK page 45, right-hand column -page 46, left-hand column	1-4

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

page 2 of 2

(27)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.

PCT/US 00/18324

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5715462 A	03-02-1998	JP 7281934 A	27-10-1995
		CN 1127043 A	17-07-1996
		DE 19580589 T	27-06-1996
		GB 2294568 A, B	01-05-1996
		WO 9527941 A	19-10-1995
		KR 176272 B	15-05-1999

 フロントページの続き

(81) 指定国 EP (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), EA (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW

(72) 発明者 トーマス アニル フランシス
 アメリカ合衆国 ワシントン州 98052
 レッドモンド ノースイースト フィフティ
 ーフイフス ストリート 18470

(72) 発明者 ジャマル ハウルーン エム エイ
 アメリカ合衆国 ワシントン州 92846
 レッドモンド ワンハンドレッドアンドフ
 ィフティセカンド アヴェニュー ノー
 スイースト 6321

(72) 発明者 クリシュナスワミ ブリジェッシュ エス
 アメリカ合衆国 ワシントン州 98007
 ベルビュー ノースイースト サーティー
 ンス プレイス #1908 15400

Fターム (参考) 5B076 FC06
 5B082 DC05 DE07 FA16 GA14